МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Контроль безопасности автоматизированных систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 42,25
самостоятельная работа 29,75

Виды контроля в семестрах:
зачеты 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	14	14	14	14
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	42,25	42,25	42,25	42,25
Контактная работа	42,25	42,25	42,25	42,25
Сам. работа	29,75	29,75	29,75	29,75
Итого	72	72	72	72

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины является подготовка квалифицированных специалистов способных осуществить контроль безопасности информационных ресурсов и систем при катастрофах, авариях, стихийных бедствиях и их последствиях.
1.2	Задачами дисциплины являются:
1.3	изучение основ и методов поиска рациональных решений построения катастрофоустойчивых информационных систем; изучение основных подходов к обеспечению информационной безопасности катастофоустойчивых информационных систем; изучение принципов функционирования современных средств построения и аппаратно-программных платформ построения информационных систем;
1.4	приобретение студентами навыков по проектированию и реализации комплекса мер, обеспечивающих информационную безопасность в
1.5	условиях чрезвычайных ситуаций, минимизации последствий чрезвычайных ситуаций и выведения информационной системы на заданный уровень.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Защита информации от утечки по техническим каналам
2.1.2	Мониторинг информационной безопасности и активный поиск киберугроз
2.1.3	Информационная безопасность открытых систем
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Эксплуатация автоматизированных систем в защищенном исполнении

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	
Знать:	
Уровень 1	риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки; организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы; классификацию и количественные характеристики технических каналов утечки информации;
Уровень 2	способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности; организацию защиты информации от утечки по техническим каналам на объектах информатизации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах;
Уровень 3	способы обеспечения контроля безопасности автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
Уметь:	
Уровень 1	анализировать и оценивать угрозы информационной безопасности автоматизированных систем; осуществлять управление и администрирование защищенных автоматизированных систем;
Уровень 2	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; использовать средства инструментального контроля показателей эффективности технической защиты информации;
Уровень 3	осуществлять планирование, организацию и контроль над безопасностью автоматизированной системы с учетом требований по защите информации; восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;
Владеть:	
Уровень 1	навыками анализа информационной инфраструктуры автоматизированных систем; навыками разработки политик информационной безопасности автоматизированных систем;
Уровень 2	навыками проектирования системы защиты объекта информатизации от утечек по техническим каналам; навыками применения способов обеспечения контроля безопасности автоматизированных систем;
Уровень 3	навыками разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности); навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе

	электронных аппаратных средств автоматизированных систем;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы, организационную структуру и функциональную часть автоматизированных систем;
3.1.2	методы и средства реализации удаленных сетевых атак на автоматизированные системы;
3.1.3	типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации,
3.1.4	классификацию и количественные характеристики технических каналов утечки информации;
3.1.5	способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности;
3.1.6	организацию защиты информации от утечки по техническим каналам на объектах информатизации;
3.1.7	принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки
3.2	**Уметь:**
3.2.1	осуществлять диагностику и мониторинг систем защиты автоматизированных систем, осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
3.2.2	проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации, использовать средства инструментального контроля показателей эффективности технической защиты информации;
3.2.3	разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем
3.3	**Владеть:**
3.3.1	разработки политик информационной безопасности автоматизированных систем;
3.3.2	проектирования системы защиты объекта информатизации от утечек по техническим каналам;
3.3.3	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Катастрофоустойчивость в системе национальной безопасности Российской Федерации						
1.1	Национальные интересы и угрозы катастрофоустойчивости Российской Федерации в информационной сфере и их обеспечение /Лек/	8	4	ОПК-13	Л1.1Л2.1	0	
1.2	Понятие национальной безопасности; Виды защищаемой информации /Пр/	8	4	ОПК-13	Л1.1Л2.1	1	
	Раздел 2. Методы обеспечения катастрофоустойчивости автоматизированных систем						
2.1	Обеспечение катастрофоустойчивости системы /Лек/	8	4	ОПК-13	Л1.1Л2.1	0	
2.2	Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф и Оптимизация средств восстановления после отказов /Лек/	8	4	ОПК-13	Л1.1Л2.1	0	
2.3	Расчет показателей доступности информационно-телекоммуникационных систем /Пр/	8	2	ОПК-13	Л1.1Л2.1	1	
	Раздел 3. Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем						
3.1	Практические решения построения средств восстановления после катастроф /Лек/	8	4	ОПК-13	Л1.1Л2.1	0	

3.2	Основы обеспечения информационной безопасности в катастрофоустойчивых центрах обработки информации /Лек/	8	4	ОПК-13	Л1.1Л2.1	0	
3.3	Принципы построения организационно -режимных мер обеспечения безопасности информации /Лек/	8	4	ОПК-13	Л1.1Л2.1	0	
3.4	Средства обеспечения катастрофоустойчивости /Пр/	8	2	ОПК-13	Л1.1Л2.1	0	
3.5	Разработка технического задания на катастрофоустойчивые системы /Пр/	8	2	ОПК-13	Л1.1Л2.1	1	
	Раздел 4. Организация функционирования катастрофоустойчивых автоматизированных систем						
4.1	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам ИС в особых режимах ее функционирования /Лек/	8	2	ОПК-13	Л1.1Л2.1	0	
4.2	Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации /Лек/	8	2	ОПК-13	Л1.1Л2.1	0	
4.3	Организация работ по развертыванию катастрофоустойчивых решений. /Пр/	8	2	ОПК-13	Л1.1Л2.1	0	
4.4	Планы восстановления после катастроф. /Пр/	8	2	ОПК-13	Л1.1Л2.1	1	
4.5	Составление технического задание на разработку катастрофоустойчивой информационной системы /Ср/	8	29,75	ОПК-13	Л1.1Л2.1	0	
4.6	Зачет /ИВКР/	8	0,25	ОПК-13	Л1.1Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Организационная система обеспечения ИБ в Российской Федерации
1. Какова структура государственной системы обеспечения информационной безопасности?
2. Какие органы государственной власти отвечают за защиту информации в РФ?
3. Какие полномочия имеет ФСТЭК России в сфере защиты информации?
4. Какие функции выполняет ФСБ России в обеспечении информационной безопасности?
5. Как взаимодействуют между собой государственные структуры в области ИБ?
Тема 2: Виды защищаемой информации. Нормативно-правовая база
6. Какие виды информации относятся к категории защищаемой?
7. Что такое информация ограниченного доступа и как она классифицируется?
8. Какие нормативные правовые акты регулируют вопросы защиты информации в РФ?
9. Каково значение национальных стандартов ГОСТ Р в области ИБ?
10. Как законодательство регулирует защиту персональных данных и государственной тайны?
Тема 3: Понятие и задачи создания КСЗИ
11. Что понимается под комплексной системой защиты информации (КСЗИ)?
12. Какие основные цели и задачи решаются при создании КСЗИ?
13. Почему важно интегрировать различные средства ИБ в единую систему?
14. Как соотносится КСЗИ с требованиями законодательства и стандартов?
15. Какие риски можно минимизировать с помощью КСЗИ?
Тема 4: Принципы организации и этапы разработки КСЗИ
16. На каких принципах строится организация КСЗИ?
17. Какие этапы включает процесс создания комплексной системы защиты?
18. Какие роли играют технические, программные и административные меры?
19. Какие документы формируются на каждом этапе разработки КСЗИ?
20. Как осуществляется тестирование и внедрение КСЗИ?
Тема 5: Требования к документации при проектировании КСЗИ
21. Какие документы необходимы при проектировании КСЗИ?
22. Что включает политика информационной безопасности организации?
23. Как оформляются процедуры управления доступом и инцидентами?

24. Какие руководящие документы разрабатываются для сотрудников?
25. Как документируется модель угроз и план реагирования?
Тема 6: Объекты защиты и защищаемая информация
26. Как определяются объекты информатизации, требующие защиты?
27. Как классифицируется информация по степени конфиденциальности?
28. Какие данные попадают под категорию «персональные»?
29. Как определяется принадлежность информации к государственной тайне?
30. Какие факторы влияют на выбор уровня защищённости объекта?
Тема 7: Разработка модели актуальных угроз
31. Что такое модель угроз и зачем она нужна?
32. Какие источники угроз учитываются при построении модели?
33. Как оцениваются вероятность и потенциальный ущерб от угроз?
34. Как строится дерево угроз или карта рисков?
35. Как модель угроз влияет на выбор мер защиты?
Тема 8: Компоненты КСЗИ
36. Какие элементы входят в состав комплексной системы защиты информации?
37. Какие технические средства используются для защиты информации?
38. Какие организационные меры обеспечивают безопасность информации?
39. Какие программные решения применяются в КСЗИ?
40. Какие физические меры защиты информации используются?
Тема 9: Основные требования к компонентам КСЗИ
41. Какие общие требования предъявляются к средствам защиты информации?
42. Какие технические характеристики должны соответствовать требованиям стандарта?
43. Как организуется совместимость и интеграция компонентов КСЗИ?
44. Какие критерии надёжности и отказоустойчивости применяются к средствам защиты?
45. Как обеспечивается соответствие компонентов КСЗИ требованиям законодательства?
Тема 10: Обеспечение функционирования КСЗИ
46. Что входит в программно-аппаратное обеспечение КСЗИ?
47. Какие организационные мероприятия обеспечивают устойчивость системы?
48. Какие материально-технические средства используются в КСЗИ?
49. Как обеспечивается кадровое сопровождение системы защиты?
50. Как проводится обучение персонала вопросам информационной безопасности?
Тема 11: Моделирование системы управления КСЗИ
51. Как строится модель системы управления КСЗИ?
52. Какие подходы используются для анализа состояния системы?
53. Какие метрики используются для оценки эффективности управления?
54. Как организуется система мониторинга и анализа событий безопасности?
55. Какие механизмы ответственности и контроля внедряются?
Тема 12: Методы оценки эффективности КСЗИ
56. Какие методы используются для оценки эффективности КСЗИ?
57. Как рассчитывается уровень защищённости информации?
58. Какие показатели используются при анализе эффективности защиты?
59. Как проводится внутренний и внешний аудит КСЗИ?
60. Какие выводы делаются на основе результатов оценки?
Тема 13: Управление КСЗИ в чрезвычайных ситуациях
61. Какие типы чрезвычайных ситуаций могут повлиять на информационную безопасность?
62. Как организуется система реагирования на инциденты ИБ?
63. Как разрабатывается и внедряется план реагирования на ЧС?
64. Какие действия предпринимаются при утечке информации или атаке?
65. Как восстанавливается работа КСЗИ после ЧС?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Контроль безопасности автоматизированных систем" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 8 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
6.1. Рекомендуемая литература			
6.1.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Богатырев В. А.	Информационные системы и технологии. Теория надежности: учебное пособие для вузов	Москва: Юрайт, 2024
6.1.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Тумбинская М. В., Петровский М. В.	Защита информации на предприятии: учебное пособие для вузов	Санкт-Петербург: Лань, 2025
6.3.1 Перечень программного обеспечения			
6.3.1.1	Office Professional Plus 2019		
6.3.1.2	Windows 10		
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.	
6.3.2 Перечень информационных справочных систем			
6.3.2.1	База данных научных электронных журналов "eLibrary"		
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"		
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")		

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Контроль безопасности автоматизированных систем" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.